A comprehensive survey of AI-enabled phishing attacks detection techniques

Year: 2020 | Citations: 309 | Authors: A. Basit, Maham Zafar, Xuan Liu, A. R. Javed, Z. Jalil

---

Abstract

In recent times, a phishing attack has become one of the most prominent attacks faced by internet users, governments, and service-providing organizations. In a phishing attack, the attacker(s) collects the client's sensitive data (i.e., user account login details, credit/debit card numbers, etc.) by using spoofed emails or fake websites. Phishing websites are common entry points of online social engineering attacks, including numerous frauds on the websites. In such types of attacks, the attacker(s) create website pages by copying the behavior of legitimate websites and sends URL(s) to the targeted victims through spam messages, texts, or social networking. To provide a thorough understanding of phishing attack(s), this paper provides a literature review of Artificial Intelligence (AI) techniques: Machine Learning, Deep Learning, Hybrid Learning, and Scenario-based techniques for phishing attack detection. This paper also presents the comparison of different studies detecting the phishing attack for each AI technique and examines the qualities and shortcomings of these methodologies. Furthermore, this paper provides a comprehensive set of current challenges of phishing attacks and future research direction in this domain.